

Contents

1. Introduction	1
1.1 Motivation	4
1.1.1 Developing the Inductive Method	4
1.1.2 Verifying the Protocol Goals	5
1.1.3 Investigating the Protocol Principles	6
1.2 Contribution	6
1.2.1 Inductive Method	6
1.2.2 Protocol Goals	8
1.2.3 Protocol Principles	9
1.3 Notation	10
1.3.1 Presenting the Protocols	10
1.3.2 Naming the Theorems	12
1.3.3 Wording the Symbols	13
1.4 Contents Outline	14
2. The Analysis of Security Protocols	17
2.1 Formal Approaches	18
2.1.1 Abstract State Machines	18
2.1.2 Belief Logics	19
2.1.3 Constraint Programming	20
2.1.4 Provable Security	21
2.1.5 Spi-calculus	22
2.1.6 State Enumeration	23
2.1.7 Strand Spaces	24
2.2 Interpreting the Findings	25
2.2.1 TMN	25
2.2.2 Woo-Lam	26
2.2.3 Public-key Needham-Schroeder	27
2.2.4 Shared-key Needham-Schroeder	28
3. The Inductive Method	31
3.1 Isabelle	32
3.2 Theory Hierarchy	33
3.3 Agents	36

3.4	Cryptographic Keys	36
3.5	Compromised Agents	37
3.6	Messages	38
3.7	Events	38
3.8	Traces	39
3.9	Threat Model	40
3.10	Operators	43
3.11	Protocol Model	45
4.	Verifying the Protocol Goals	49
4.1	The Reliability of the Protocol Model	50
4.2	Regularity	52
4.3	Authenticity	53
4.4	Unicity	54
4.5	Confidentiality	56
4.6	Authentication	58
4.7	Key Distribution	60
5.	The Principle of Goal Availability	63
5.1	The Need for a Threat Model	64
5.2	Goal Availability	65
5.3	Past Incarnations of Goal Availability	68
5.4	Anticipating the Applications of Goal Availability	69
6.	Modelling Timestamping and Verifying a Classical Protocol	73
6.1	Modelling Guessable Numbers	74
6.2	Modelling Time	75
6.3	The BAN Kerberos Protocol	76
6.4	Modelling BAN Kerberos	77
6.5	Verifying BAN Kerberos	79
6.5.1	Reliability of the BAN Kerberos Model	79
6.5.2	Regularity	80
6.5.3	Authenticity	80
6.5.4	Unicity	81
6.5.5	Confidentiality	82
6.5.6	Authentication	83
6.5.7	Key Distribution	84
6.6	A Temporal Modelling of Accidents	84
7.	Verifying a Deployed Protocol	87
7.1	The Kerberos IV Protocol	88
7.1.1	Overview	89
7.1.2	Details	89
7.2	Modelling Kerberos IV	91
7.2.1	Basics	92

7.2.2	Authentication Phase	92
7.2.3	Authorisation Phase	92
7.2.4	Service Phase	93
7.2.5	Accidents	93
7.3	Verifying Kerberos IV	94
7.3.1	Reliability of the Kerberos IV Model	96
7.3.2	Regularity	97
7.3.3	Authenticity	98
7.3.4	Unicity	100
7.3.5	Confidentiality	100
7.3.6	Authentication	106
7.3.7	Key Distribution	109
8.	Modelling Agents' Knowledge of Messages	111
8.1	Agents' Knowledge via Trace Inspection	112
8.1.1	Basic Lemmas	113
8.1.2	Proving Knowledge	113
8.2	Agents' Knowledge via Message Reception	114
8.2.1	From Spy's Knowledge to Agents' Knowledge	115
8.2.2	Updating the Existing Models	116
8.2.3	Basic Lemmas	118
8.2.4	Updating the Existing Theorems	118
8.2.5	Proving Knowledge	119
8.3	Revisiting the Guarantees on BAN Kerberos	119
8.3.1	Using Trace Inspection	120
8.3.2	Using Message Reception	122
8.4	Revisiting the Guarantees on Kerberos IV	124
8.4.1	Using Trace Inspection	124
8.4.2	Using Message Reception	126
8.5	Comparing the Two Approaches	130
8.5.1	On Otway-Rees and Otway-Rees-Bella	131
8.5.2	On Public-key Protocols	134
8.6	Timestamps Versus Nonces on the Same Design	135
8.6.1	Informal Account	135
8.6.2	Formal Account	136
9.	Verifying Another Deployed Protocol	139
9.1	The Kerberos V Protocol	140
9.2	Modelling Kerberos V	140
9.3	Verifying Kerberos V	143
9.3.1	Main Guarantees	143
9.3.2	Novel Proof Methods	144
9.3.3	Novel Guarantees	148

10. Modelling Smartcards	153
10.1 Smartcards	154
10.1.1 Card Vulnerabilities	155
10.1.2 Card Usability	156
10.1.3 Card Secrets	157
10.2 Events	158
10.3 Agents' Knowledge	159
10.4 Threat Model	162
10.5 Protocol Model	163
11. Verifying a Smartcard Protocol	165
11.1 The Shoup-Rubin Protocol	166
11.2 Modelling Shoup-Rubin	167
11.2.1 Basics	169
11.2.2 Phase I	169
11.2.3 Phase II	170
11.2.4 Phase III	170
11.2.5 Phase IV	171
11.2.6 Phase V	172
11.2.7 Phase VI	172
11.2.8 Phase VII	173
11.2.9 Threats	173
11.2.10 Accidents	174
11.3 Verifying Shoup-Rubin	175
11.3.1 Reliability of the Shoup-Rubin Model	176
11.3.2 Regularity	180
11.3.3 Authenticity	180
11.3.4 Unicity	184
11.3.5 Confidentiality	185
11.3.6 Authentication	188
11.3.7 Key Distribution	189
11.4 Verifying Shoup-Rubin-Bella	190
12. Modelling Accountability	195
12.1 Challenges for Formal Analysis	196
12.1.1 Formalising and Verifying the Novel Goals	196
12.1.2 Challenges from Higher-Level Protocols	197
12.2 Facing the Challenges	200
12.2.1 Formalising and Verifying the Novel Goals	200
12.2.2 Formalising the Underlying Protocols	202
12.2.3 Formalising a Threat Model	205

13. Verifying Two Accountability Protocols	207
13.1 The Non-repudiation Protocol	208
13.1.1 Model	209
13.1.2 Verification	210
13.2 The Certified E-mail Protocol	215
13.2.1 Model	217
13.2.2 Verification	218
13.3 Discussion	222
14. Conclusions	225
14.1 Statistics	229
14.1.1 Theory File Sizes	229
14.1.2 Proof Runtimes	230
14.1.3 Human Effort	232
A. Proof Script Fragments for Kerberos IV	235
A.1 Reliability	235
A.2 Session-key Compromise	237
A.3 Session-key Confidentiality	239
B. Proof Script Fragments for Kerberos V	245
B.1 Unicity	245
B.2 Unicity Relying on Timestamps	246
B.3 Key Distribution and Non-injective Agreement	249
C. Proof Script Fragments for Shoup-Rubin	253
C.1 Function “initState”	253
C.2 Function “knows”	254
C.3 Authentication	255
D. Proof Script Fragments for Zhou-Gollmann	259
D.1 Validity of Main Evidence	259
D.2 Validity of Subsidiary Evidence	260
D.3 Fairness	262
Bibliography	265